OIT OPERATIONAL PROCEDURE

Title: LOG FILE RETENTION POLICY

Identification: OIT 2
Page: 1 of 1
Effective Date: March 24, 2015
Signature/Approval: [Signature]

PURPOSE

This procedure establishes a process for retaining log files for servers and network devices managed by the college’s Information systems department.

PROCEDURE

Technology based events or activity records are collectively referred to as “logs”. These logs are generated by many sources, including security software (such as antivirus software, firewalls, and intrusion detection and prevention systems), operating systems on servers, networking equipment, and software application systems. Log retention management is essential to ensure that these records are stored in sufficient detail for an appropriate period. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems.

College’s Office of Information Technology (OIT) department will identify and maintain a list of servers, software systems, and network devices for log retention. The logs generated by these systems will be aggregated into college’s central log management system on a regular frequency.

The logs used to identify security incidents, policy violations, fraudulent activity, and operational problems will be retained for minimum period of 90 days. The maximum retention period for these logs will be one (1) year. The logs may be deleted after the retention period is over.

In cases of ongoing investigations, the college will retain the logs until the investigation is concluded and the logs are no longer needed. In addition, in case a subpoena, discovery motion, or other legal notice is received the logs cannot be destroyed. Such destruction should also be postponed if the logs might be needed for an imminent legal action.

The College’s OIT department will maintain a central log management system.

HISTORY: New